



**Kaspersky
Security
Awareness**

Gamified Assessment Tool

kaspersky

Learn more on
kaspersky.com

Gamified Assessment Tool

Kaspersky Gamified Assessment Tool (GAT): a quick and exciting way to assess employees' cybersecurity skills.

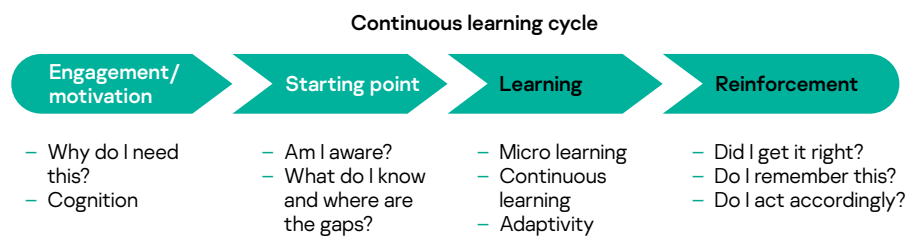
52% of enterprise organizations and 50% of SMB experienced cybersecurity incident as a result of inappropriate IT resource use by employees*

42% of business indicate employees as a most concerning IT security issue (with inappropriate IT resource use, losing company owned devices and falling victim to phishing and/or social engineering attacks)*

\$ 1195 K the average financial impact of a data breach caused by inappropriate IT resource use by employees*

Strong cybersecurity is one of the most important, yet weak, areas of many companies today. Companies around the world are working hard on cybersecurity, developing increasingly complex and efficient protection systems. Yet there remains a hole in the cybersecurity fabric of every single company that cannot be fixed by technical measures.

This gap is "the human factor". The human factor is one of the main causes of cybersecurity incidents. Changing employee behavior can be a challenge. People are not interested in learning cybersecurity: they have low motivation and often they do not even realize that they have gaps in their knowledge. How to increase employees' motivation for training? How to evaluate their current level of cybersecurity knowledge? The Gamified Assessment Tool quickly measures the current level of employees' cybersecurity skills, engaging and motivating them for further learning. The CIO/HR departments can understand the overall situation with cybersecurity awareness in the company using a short gamified tool as an introductory step to an education program.



What does the Gamified Assessment Tool offer?

- There are three scenarios for the assessment representing familiar situations that deal with specific cybersecurity skills: Working in open space, While travelling, and the Home office
- Each employee gets a scenario with 12 random situations that deal with specific cybersecurity skills. Employees should go through all of them, assessing whether the character's actions are risky or not and expressing the level of confidence in their response using chips. For each answer, the user earns a certain number of points. When calculating user's final score, the system takes into the consideration both the answer, whether it's right or wrong, and the confidence level.
- To prevent cheating and make the assessment more interesting scenario types are provided to employees randomly. 12 situations for each scenario are also randomly chosen from the library of 225 which means that fellow users will have different scenarios for evaluation.
- After users complete all the zones, they get the overall score that is an assessment of their cybersecurity awareness level and feedback on every zone, with explanations and useful tips.
- On completion of the assessment, a certificate is awarded. It can be downloaded and shared.
- Administrator of the assessment gets a report of all the users with the detailed results on every topic including scores, number of right answers and confidence level. This clear feedback on employees' level of cybersecurity competence helps to plan and set up further security awareness training more effectively.

* Report: "IT security economics in 2019", Kaspersky

Security domains covered in the Gamified Assessment Tool:

- Passwords and accounts
- Email
- Web browsing
- Social networks & Messengers
- PC security
- Mobile devices

Learning process

At the beginning of the assessment, a brief description of the rules is provided.



Within 10 minutes employees need to assess the characters' actions in 12 cybersecurity-related situations represented in the scenario. They need to decide whether the character's actions are risky or not and express the level of confidence in their response. There is a possibility to pause a game. If you need to attend to something else, don't forget to pause the game (the pause button is on the upper right corner near the timer).



Users put **green chips** if they think it's safe, or **red chips** if they think it's dangerous. The number of chips indicates how confident they are in their answer.



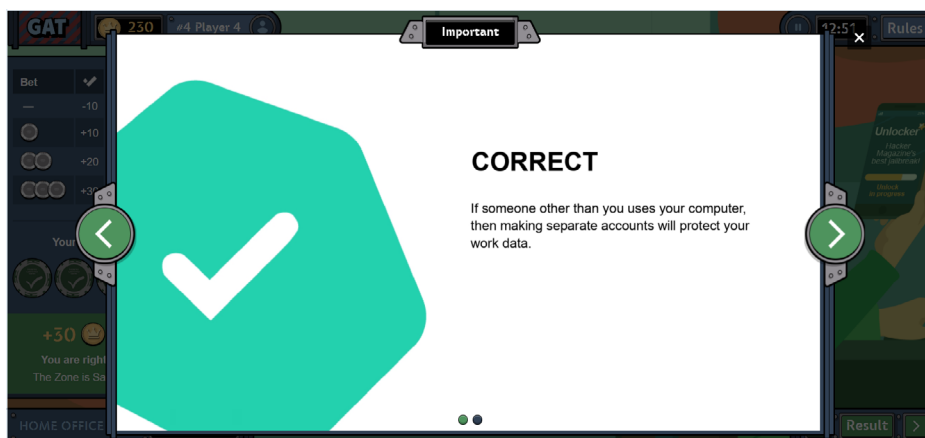
After users finish the game, they get their overall score which is an assessment of their cybersecurity awareness level.



It's possible to go through each situation.



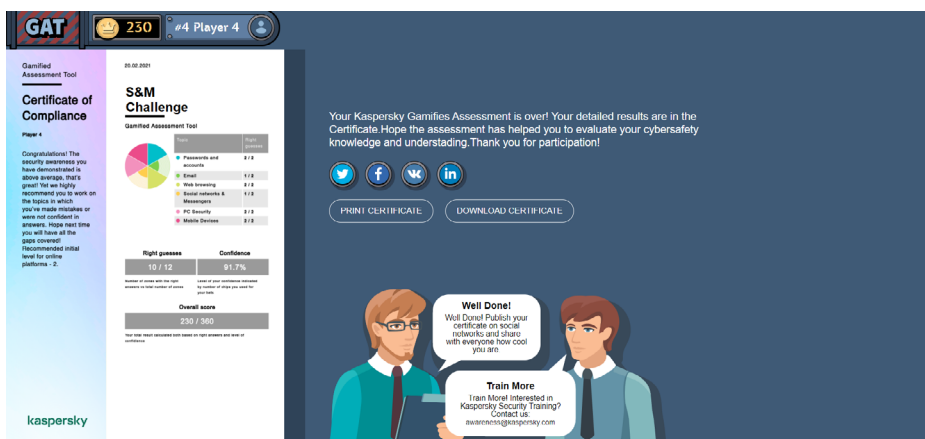
And get feedback on every zone, with explanations and tips.



A certificate with the results recommendations on which cybersecurity topics require special attention and improvement and tips for further security awareness training will be available at the end of the assessment. It can be downloaded and shared.

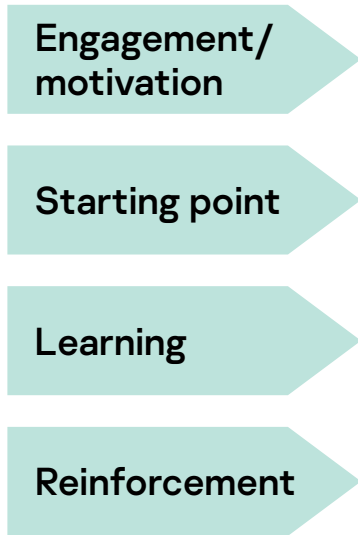
Technical recommendations

OS:
 Windows 7, 10;
 Mac: Sierra, High Sierra, Mojave, Catalina;
 Ubuntu 18.04.
 We highly recommend use browser:
 Firefox 70 and higher;
 Chrome 80 and higher;
 Safari 11 and higher.
 As a cloud solution, GAT requires only a browser on a desktop or tablet PC with a resolution of 1024x768 or higher.



Kaspersky Security Awareness – a new approach to mastering IT security skills

Kaspersky Security Awareness offers a range of highly engaging and effective training solutions that boost the cybersecurity awareness of your staff so that they all play their part in the overall cybersafety of your organization. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle that includes multiple components.



Key program differentiators



Substantial cybersecurity expertise

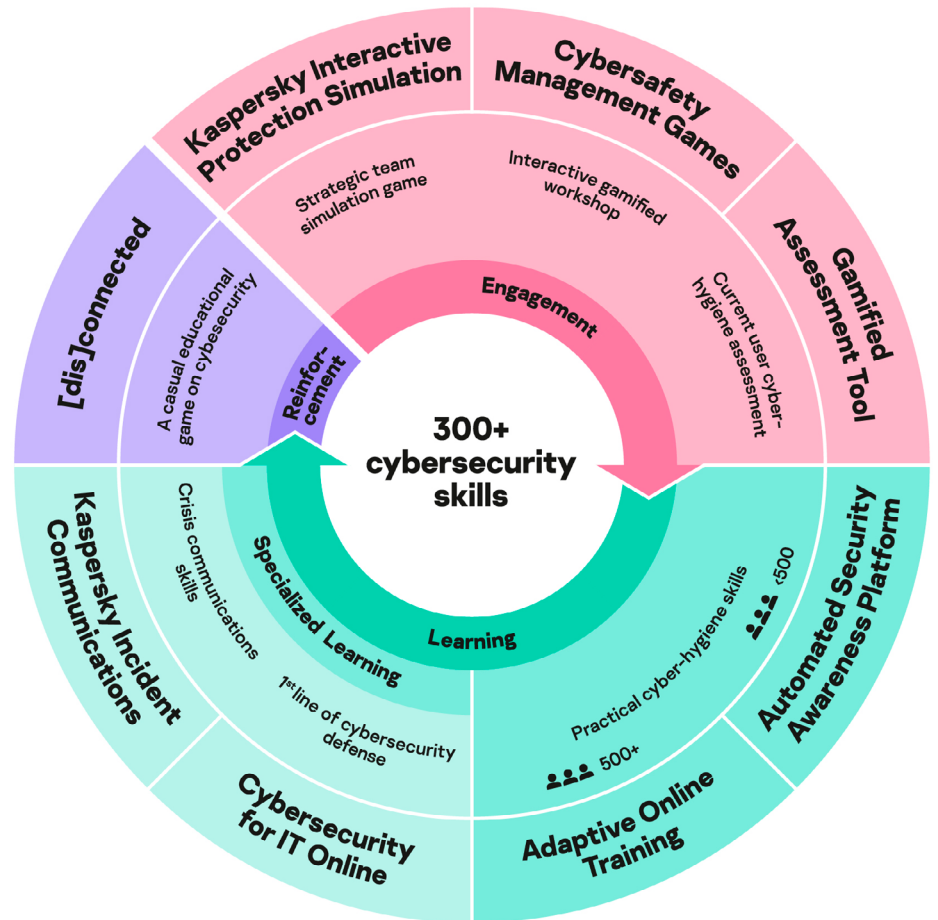
20+ years' experience in cybersecurity transformed into a cybersafety skillset that lies at the heart of our products



Training that change employees' behavior at every level of your organization

Our gamified training provides engagement and motivation through edutainment, while the learning platforms help to internalize the cybersecurity skillset to ensure that learnt skills don't get lost along the way.

Different training formats for different organizational levels



Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness

www.kaspersky.com

kaspersky BRING ON
THE FUTURE